

(19) Japan Patent Office (JP)

**(12) Published Japanese Translations of PCT International
Publication for Patent Application (A)**

(11) Patent Application Publication Number: P2003-509969A

(43) Publication Date: March 11, 2003

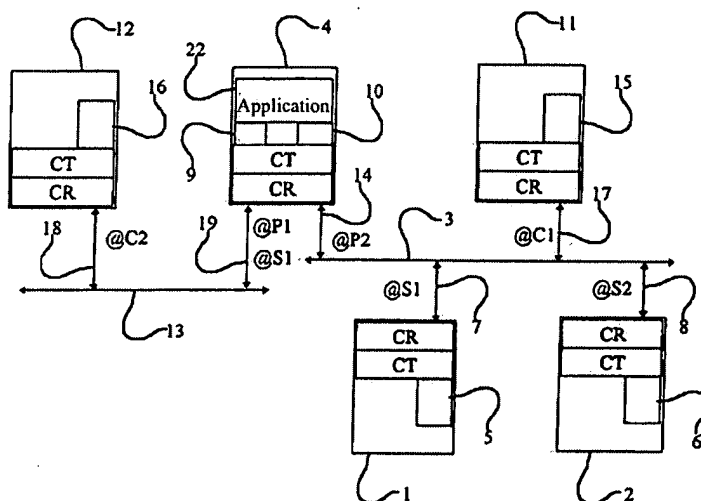
(51) International Patent Classification ⁷	Identification Number	FI	Theme Code
H04L 12/46	100	H04L 12/46	100Z 5K033

(21) Patent Application Number: P2001-524324	(81) Designated State: EP (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), CN, JP, KR, SG, US, VN
(86) (22) Application Date: 7 September 2000	(71) Applicant: Bull SA 68, route de Versailles 78430 Louveciennes, France
(85) Translation Submission Date: 15 May 2001	(72) Inventor: Dujonc, Jean-Yves 14 bis, avenue Pasteur 78580 Maule, France
(86) International Application Number: PCT/FR00/02469	(72) Inventor: René Martin 32 rue Gomez 91440 Bures-sur-Yvette, France
(87) International Publication Number: WO01/020870	(74) Agents: YOSHIO, Kawaguchi (patent attorney), et al
(87) International Publication Date: 22 March 2001	F-term (reference) 5K033 BA04 CB09 DA05 DB19 EC03
(31) Claim of Priority Number: 99/11594	
(32) Priority Date: 16 September 1999	
(33) Country Claiming Priority: France (FR)	

(54) Title: ACCESS RELAY TO THE SERVER NETWORK, WHICH IS TRANSPARENT TO THE CLIENT NETWORK

(57) Abstract: This invention relates to the interconnection device 4, which is connected to the client network 13 with the first physical interface 19 and to the server network 3 with the second physical interface 14. Interconnection device 4 includes the first relay application 22 that receives the datagram from client network 13 addressed to server devices 1 and 2 while sending the datagram addressed to server devices 1 and 2 to server network 3. Inter-network protocol addresses @S1 and @S2 for server devices 1 and 2, which connect to the server network 3, are associated with the first physical interface 19. Therefore, the datagram that gets back to the application level on the interconnection device is provided to the relay application transparent to client network 13.

Fig.1



[Claim(s)]

[Claim 1] An interconnection device (4), which is characterized by the inclusion of the first relay application (22) that receives the datagram addressed to server devices (1, 2) from the client network (13) and sends the datagram addressed to server devices (1, 2) to the server network (3). It is connected to the client network (13) with the first physical interface (19) and is connected to the server network (3) with the second physical interface (14), and at least one inter-network protocol address (@S1, @S2) for server devices (1, 2) that is different from the interconnection device (4) is associated with the first physical interface (19).

[Claim 2] An interconnection device (4), which is characterized by the inclusion of the first relay application (22) that receives the datagram addressed to server devices (1, 2) from the client network (13) and sends the datagram addressed to server devices (1, 2) to the server network (3). It is connected to the client network (13) with the first physical interface (19) and is connected to the server network (3) with the second physical interface (14), and at least one inter-network protocol address (@S1, @S2) for server devices (1, 2) that is different from the interconnection device (4) is associated with the first physical interface (19) and the third physical interface (2), which is different from the second physical interface (14).

[Claim 3] An interconnection device (4) according to Claim 1, which is characterized by the fact that the aforementioned address (@S1, @S2) is associated with the first physical interface (19) as the address synonymous to the base address (@P1) of the interconnection device (4) on the client network (13).

[Claim 4] A method that executes the relay application (22) between the client network (13) and the server network (3) on the interconnection device (4) and enables the client application (16) to process the datagram that is sent to the server device (1) of the address (@S1) on the server network (3) that is different from the interconnection device (4) using the said relay application. It is a method that is characterized by the inclusion of the first step that associates the aforementioned address (@S1) to the physical interface (19, 20) of the interconnection device (4), which is not connected to the server network (3), so that the relay application (22) will receive the aforementioned datagram without sending data to the aforementioned client application (16) or constructing the said client application so that it can process the datagram.

[Claim 5] The method according to Claim 4, which is characterized by the fact that the first step is preceded by the second step that routes the datagram, which is transmitted to the server device (1) on the client network (13), to the interconnection device (4).

[Claim 6] The interconnection device (4) according to Claim 1 or 2, which is characterized by the possession of an encryption key, which enables the relay application (22) to decrypt and transmit the encrypted message sent by the client network (13) on the server network (3).

[Claim 7] The interconnection device (4) according to Claim 1 or 2, which is characterized by the inclusion of an encryption key that enables the relay application (22) to encrypt and send unencrypted messages that are sent from the server network (3) on the client network (13).

[Detailed Description]

[0001]

This invention relates to the field of the information processing network. An information processing network enables execution of applications distributed on remote devices. These remote devices are connected to the same network or to different multiple networks that are interconnected by the interconnection unit.

[0002]

Transactions between remote devices are initialized by the client application, which sends a request message to the server application, which is in monitoring state. Client application then goes into standby state, which waits for a response message to the request message. Once it receives the request message, the server application generates a response message to send to the client application. Network layer can transport each message as datagram, from the device that contains the transmitting application to the device that contains the receiving application. Transport layer can transport a message first between the transmitting application and the network layer and second between the network layer and the receiving application, such as from a client application to a server application, for example. Application layer is related to the execution of applications in an environment unique to the layer.

[0003]

If the devices are not connected to one physical network, the routing protocol in the network layer sends the datagram from the transmitting device to the interconnecting device and from the interconnecting device to the receiving device using an inter-network protocol address, such as an IP address. Datagram remains in the network layer when it passes through the interconnecting device. The network between the client device and interconnecting device is called the client network. The network between the server device and the interconnecting device is called the server network.

[0004]

The technical scope that this invention involves in particular is related to the interconnection device (proxy) that contains the relay application. The relay application is effective in processing the messages exchanged between the client and server networks. However, the datagram addressed to the final receiving device does not get back to the application layer of the interconnection device.

[0005]

According to known prior art, the transmitting application does not directly address the final receiving application but rather addresses the relay application in the interconnection device and indicates the final receiving application in the message to the relay application so that the relay application can re-transmit the message. This is done on an Internet browser (browser), for example. On a browser, the address of the interconnection device for the network layer and the port number of the relay application for the transport layer can be declared against the designated client application. Therefore, the browser encloses the address of the server device and the port number of the final receiving application in the datagram addressed to the relay application. For this, however, the relay application through which the message passes must be clear so that the corresponding client device can be configured. As a result, this system lacks flexibility. Lack of flexibility may be within tolerable range for a limited number of applications but not for a large number of different applications.

[0006]

Document RFC1928, which can be obtained at the Internet address <http://www.pmg.lcs.mit.edu/cgi-bin/rfc/view?1928>, describes the protocol "SOCKS v5." The SOCKS program is conventionally located on port 1080. With a solution

called "TCP Protocol Tunneling in Web Proxy Servers," too, the first connection to the relay application must be configured, and then the second connection that connects to the relay device as the final device must be configured.

[0007]

In order to resolve the problem described above, the goal of this invention is to simplify the configuration of the connection between the client application to the server application, so as to be used when the client application does not use the relay application service. That is, to make the use of the relay application service transparent to the client application.

[0008]

The first goal of this invention is in the interconnection device, which is connected to the client network with the first physical interface and to the server network with the second physical interface. It is characterized by the inclusion of the first relay application, which receives the datagram sent from the client network to a server device and sends it to the server network, while at least one inter-network protocol address of the server device connected to the server network is associated with the first physical interface.

[0009]

As a result, once the datagram reaches the first physical interface that is equipped with the inter-network protocol address of the server device as the destination address, the interconnection device is recognized as the destination device of the datagram by its network layer. In that case, the network layer of the interconnection device extends the datagram back towards the application layer of the interconnection device by simply complying with the predefined protocol. Once the relay application receives the datagram, it processes the datagram and may or may not resend it to the server device. This is perfectly transparent to the client application.

[0010]

The goal of the modified implementation format of this invention is in the interconnection device, which is connected to the client network with the first physical interface and to the server network with the second physical interface. It includes the first relay application, which receives the datagram sent from the client network to a server device and sends it to the server network, while at least one inter-network protocol address of the server device connected to the server network is associated with

a third physical interface, which is different from the first or second physical interface.

[0011]

Here, the protocol on the network layer allocates the destination address not to the first physical interface that receives the datagram but to an arbitrary physical interface of the interconnection device so that it gets back towards the application layer of the interconnection device.

[0012]

If, for example, the interconnection device already has a valid base address for a routine protocol on the client network, the aforementioned address of the server device is associated with the first physical interface on the client network as an address synonymous to the base address of the interconnection device.

[0013]

The second goal of this invention is the method that enables the client application to process the datagram that is sent to a server device that has one address on the server network on the client network using a relay application, which is executed between the client network and the server network on the interconnection device. It is characterized by the fact that the physical interface of the interconnection device that is not connected to the server network includes the first step that associates the aforementioned address on the server network, so that the relay application receives the aforementioned datagram.

[0014]

This method has an advantage, which is the fact that the relay application does not need to configure the aforementioned client application in order to enable the relay application to process the datagram, nor does it need to communicate with the aforementioned client application. In fact, the client application continues to send the datagram using the address of the server device. Once the datagram reaches the first physical interface of the interconnection device, the network protocol naturally ensures that the datagram gets up towards the application layer of the interconnection device. That enables the relay application to receive the datagram.

[0015]

When the datagram, which is sent from the client network to the server network, must

be routed by the interconnection device, this method is characterized by the fact that the second step, which routes the datagram sent from the client network to the server device to the interconnection device, precedes the first step. This happens, for example, when the number of interconnection device between the client network and server network is not limited to one.

[0016]

Other advantages and details of the implementation format of this invention will become clear from the following description to the attached drawings.

[0017]

Drawing 1 shows server devices 1 and 2 and client devices 11 and 12. Devices 1, 2, and 11 are connected to server network 3 with physical interfaces 7, 8, and 17, respectively. Client device 12 is connected to client network 13 with physical interface 18. Networks 3 and 13 are physically different. Interconnection device 4 is connected to server network 3 with physical interface 14 and to client network 13 with physical interface 19.

[0018]

Applications 5, 6, 15, and 16, which are executed on devices 1, 2, 11, and 12, respectively, communicate with one another in the transport layer CT in connectionless mode, such as UDP, or in connection mode, such as TCP, based on the protocol. Transport layer CT monitors the network layer CR based on the protocol, such as IP.

[0019]

In the network layer CR, device 1 is recognized by address @S1, device 2 is recognized by address @S2, and device 11 is recognized by address @C1. As it is known, each address, @S1, @S2, and @C1, has a network field, which has a common value that identifies network 3, and a device field, which has separate values that identify the devices that are connected to network 3. Device 12 is recognized by @C2, the address that has the network field value that identifies network 13 and the device field value that identifies device 12 on network 13. Interconnection device 4 is recognized by @P1, the address that has the network field value that identifies network 13 and the device field value that identifies the interconnection device 4 on network 13, and by @P2, the address that has the network field value that identifies network 3 and the device field value that identifies the interconnection device 4 on network 3.

[0020]

The devices communicate with one another with messages that circulate the network as datagram. Drawing 2 shows an example of a datagram. This datagram, which is a bit frame sequence, mainly consists of three consecutive fields. First field DR is for the network layer protocol. Second field DT is for the transport layer protocol, which monitors the network layer. Third field DA is for the application layer that monitors the transport layer. For a web request, for example, field DR contains the sender's and recipient's IP addresses, field DT contains the sender's and recipient's TCP port numbers, and field DA contains the HTTP data.

[0021]

For example, if client application 15, which is executed on client device 11, executes an access request to the file that is processed by the server application 5, which is located on server device 1, application 5 sends the request to layer CT of client device 11, and the layer CT writes the request to field DA, while writing the service port number for application 15 and service port number for application 5 to field DT. Layer CT of client device 11 sends fields DT and DA to layer CR of device 11. Layer CR writes @C1, the address of client device 11 and @S1, the address of server device 1, to field DR. Next, the layer CR sends the datagram, which consists of data as described above, to interface 17, which reaches interface 7 of server device 1. Layer CR of server device 1 recognizes that the datagram is addressed to the upper layer of server device 1 from the address @S1 and sends the fields DT and DA to layer CT of device 1. Layer CT resends the field DA to application 5 based on the service port number of application 5, and finally, application 5 processes the request.

[0022]

For example, if client application 16, which is executed on client device 12, executes an access request to the file that is processed by application 5, which is located on server device 1, application 16 sends the request to layer CT of client device 12. Layer CT writes the request to field DA, while writing the service port number for application 16 and service port number for application 5 to field DT. Layer CT of client device 12 sends fields DT and DA to layer CR of client device 12. Layer CR writes client device 12's address @C2 and server device 1's address @S1 to field DR. Next, layer CR sends the datagram, which consists of data as described above, to interface 18, which arrives at interface 19 of the interconnection device 4, which is declared as the router between networks 13 and 3.

[0023]

If there is no device by this invention, layer CR of interconnection device 4 recognizes that the datagram is not addressed to the upper layer of interconnection device 4 because address @S1 is not an address for interconnection device 4. In that case, layer CR of interconnection device 4 searches for the line in the routing table that contains the same value as the network field of address @S1. The line that is found indicates interface 14 as the access interface to network 3. Layer CR of the interconnection device 4 resends the datagram to network 3 using interface 14. As a result, the datagram reaches interface 7 of the server device 1. Layer CR of server device 1 recognizes that the datagram is addressed to the upper layer of server device 1 from address @S1 and resends fields DT and DA to layer CT of server device 1. Layer CT resends the field DA to application 5, based on the server port number for application 5, and finally, the application processes the request.

[0024]

With a device of this invention, interconnection device 4 contains application 22, which works as a proxy server for the request that is sent from network 13. Application 22 has multiple advantages. For example, it can restrict access to devices 1, 2, and 11 that are connected to server network 3. It also protects the responses to preceding requests, which is stored in cache memory, and can reproduce responses to new requests without sending new requests to the server devices 1 and 2.

[0025]

Multiple addresses of layer CR are associated with the physical interface 19, regular address @S1, and @P1, the regular address of server device 1, which is connected to network 3. Address @S2 of server device 2 can be attached to physical interface 19. As more fully discussed hereinafter, with this method, the server network determines the service usage of relay application 22, such as its access to server 1, for example, by associating address @S1 with physical interface 19, unlike prior art, in which the client network determines the service usage of the relay application 22.

[0026]

Application 22 includes input port 9, which has the same number as the input port of application 5, and output port 10. Any arbitrary request message addressed to application 5 can be managed by allocating one number to this output port.

[0027]

Thanks to such special devices, client device 12 does not need to know that intermediary connection with interconnection device 4 has been established. When application 16, which is executed on client device 12, executes a request that is addressed to application 5, which is located on server device 1, address @S1 is now recognized by network 13 as the address of interconnection device 4.

[0028]

Application 16 sends datagram Q on network 13, in order to execute the request addressed to application 5. Datagram Q contains addresses @S1 and @S2 in the field CR, port numbers for applications 5 and 16 in the transport field, and the final information addressed to application 5 in field CA.

[0029]

Once physical interface 19 of interconnection device 4 receives datagram Q, the network layer CR of interconnection device 4 recognizes the destination address @S1 in field DR as a unique address and gets the datagram up to the transport layer CT of interconnection device 4. Transport layer CT recognizes the destination number in field DT as port number 9 of application 22 and sends the content of datagram Q to this application.

[0030]

Application 22 processes the content of field DA of datagram Q. Processing of datagram Q by application 22 includes checking the access rights and checking if interconnection device 4 already has a response to the request in its cache memory, in order to determine whether datagram Q must be sent to server application 5.

[0031]

If application 22 needs to send a request message to application 5 so that it can process the request message sent from client application 16, application 22 notifies the transport layer CT of interconnection device 4 of the subsequent data, which is the content of the request placed in field DA, input port number of application 5, output port number of application 22, which is used to manage the responses to requests, and @S1, the inter-network protocol address of server device 1. These data are sent to the network layer CR of interconnection device 4. Once the network layer CR of

interconnection device 4 receives these data, it looks for the network on which the datagram will be sent, in the routing table based on the network field of the address @S1. In the example provided here, layer CR sends the datagram that contains the destination address @S1 and the sender address @P2, which is associated with physical interface 14, in field DR, to physical interface 14, for the network field of the address @S1 corresponds to network 3 to which server device 1 is connected. The datagram reaches server device 1 and its server application 5 on client server 3 using the conventional method.

[0032]

Response that application 5 receives on interface 14 is sent up to application 22 by the network layer because the address @P2 is the address for interconnection device 4. It is sent up to application 22 by the transport layer CT because the port number for the response is the number that application 22 allocates to port 10. Using an internal mechanism that manages requests and responses, application 22 associates the response to the output port number received from application 16. Application 22 notifies transport layer CT of the interconnection device 4 of the subsequent data, which is the content of the request placed in field DA, output port number of application 16, input port number of application 22, which is the same as the input port number of application 5 in order to manage the responses to requests, @C2, which is the destination inter-network protocol address of client device 12, and @S1, which is the sender inter-network protocol address of server device 12. These data are sent to the network layer CR of interconnection device 4. Once the network layer CR of interconnection device 4 receives these data, it looks for the network on which the datagram will be sent, in the routing table based on the network field of the address @C2. In the example provided here, layer CR sends the datagram that contains the destination address @P2 and the sender address @S1, which is associated with physical interface 19, in field DR, to physical interface 19, for the network field of the address @C2 corresponds to network 13 to which client device 12 is connected. The datagram reaches client device 12 and its server application 16 on client network 13 using the conventional method.

[0033]

As a result application 16 on client device 12 returns the response from application 5 in server device 1 without passing through application 22. Passage of application 22 is done transparently to client application 16.

[0034]

As seen in drawing 3, address @S1 is associated with interface 14, as described above, and here especially to physical interface 20, which is different from interface 19.

[0035]

Once the datagram is sent on network 13 with the address @S1, routing protocol of the network layer of interconnection device 4 receives the datagram on interface 19 with which address @P1 is associated. Since address @S1 associated with physical interface 20 is the address of the interconnection device 4, datagram gets up to application layer CA of interconnection device 4.

[0036]

Relay application 21 processes the request message sent from the received datagram, just like relay application 22, as described previously. Relay application 22 especially provides a pilot to the virtual network to which physical interface 20 is connected, in order to send the response message to client device 12.

[0037]

Implementation of this invention becomes particularly simpler when the IP address @S1 is connected to interface 19. In the following simple example, application 16 executes the Telnet function as a client application, and relay application 22 executes telnetd as the server application of application 16 and Telnet as the client of application 5. Application 5 executes telnetd as the server of relay application 22. Telnet and telnetd connect the terminal of the client device on which Telnet is executed to the server device on which telnetd is executed. This is a known function that uses TCP/IP.

[0038]

Each device goes to a different operation system to follow the device that executes the command. Client device 12 goes to an AIX system (registered trademark) version 4.1 and has an IP address of @C1 = 129.182.51.18. Relay device 4 goes to an AIX system version 4.2 and has an IP address of @P1 = 129.182.51.21 and @P2 = 192.90.249.22. Server device 12 goes to a DNS-E device (dedicated) and has an IP address of @S1 = 192.90.249.124. Network 13 can be accessed by a known method with an IP address @R1 = 129.182.50, mask @M1 = 255.255.254.0.

[0039]

On client device 12, the following command *route add-host 192.90.249.124 129.182.51.21* determines that the sent datagram passes through the relay device with the address @P1 in order to reach the server device 1 with the address @S1.

[0040]

On server device 1, the following command *route add-net 129.182.50 192.90.249.22-netmask 255.255.254.0* determines that the sent datagram passes through the relay device with the address @P2 in order to reach all devices on network 13 with the address @R1.

[0041]

On client device 12, the following command *Telnet 192.90.249.124* launches the Telnet application in order to reach server device 1 with the address @S1. At this point, the only device that can be recognized by the IP address @S1 is server device 1. The IP layer of interconnection device 4 routes the datagram sent from the IP layer of client device 12 towards the IP layer of server device 1. IP layer of server device 1 recognizes the address @S1 and walks back the datagram's application field towards the telnetd application of server device 1. Telnetd application of server device 1 sends the following message to client device 12 on its way back:

Trying...

Connected to 192.90.249.124.

Escape character is '^'.

*\$\$ 0000 *DNS-E V3U1.000 P1.001 P2.019 P3.010*IMA:BX77SIM 1988/10/21 17:23**

[0042]

The above message indicates that the message is in a DNS system environment; that is that it reaches server device 1 directly. It is only when IP routing is executed that it passes through relay device 4.

[0043]

On client device 12, the following command *Telnet 129.182.51.21* launches the Telnet application in order to reach the relay device 4 with the address @P1. The IP layer of interconnection device 4 recognizes the address @P1 and walks back the datagram's application field towards the telnetd application on relay device 4. Telnetd application

of interconnection device 4 sends the following message to client device 12 on its way back:

```
Trying...
Connected to 129.182.51.21.
Escape character is '^'.
Telnet (treize)
AIX Version 4
(c) Copyrights by IBM and by others 1982, 1996
Login:
```

[0044]

Display of the above message on the terminal of client device 12 indicates that the message is in an AIX system; that is, that it reaches interconnection device 4. With this, commands from the terminal of client device 12, which are executed on interconnection device 4, can be managed.

[0045]

On interconnection device 4, interface 19 is named en1, and the following command *ifconfig en1 192.90.249.124.alias* determines the address @S1 as an additional address associated with interface 19. There is no danger that interconnection device 4 is confused with server device 1 by the IP layer on network 13. This is because network 13 is physically different from network 3. Also, the following command *ifconfig en1 192.90.249.125.alias* determines the address @S2 as an additional address associated with interface 19.

[0046]

Back on client device 12, the following command *Telnet 192.90.249.124* launches a Telnet application that has an effect different from the one noted above. The following message is displayed on the terminal of client device 12:

```
Trying...
Connected to 129.182.51.21.
Escape character is '^'.
Telnet (treize)
AIX Version 4
```

(c) Copyrights by IBM and by others 1982, 1996

Login:

[0047]

Display of the above message on the terminal of client device 12 indicates that the message is in an AIX system of interconnection device 4. Even though connection to the telnetd application on server device 1 was requested using the address @S1, the command executed the connection to telnetd application on server 4. This can be explained by the fact that the IP layer of interconnection device 4 recognized address @S1 as the unique destination address to interconnection device 4 without considering routing it to network 3. Therefore, the IP layer of interconnection device 4 walks back the application field of the datagram that was received on interface 19 towards the telnetd application on interconnection device 4.

[0048]

On interconnection device 4, the following command *Telnet 192.90.249.124* launches a Telnet application in order to reach server device 1 with the address @S1. At this point, the only device that can be recognized by the IP address @S1 by interface 14 is server device 1. The IP layer of server device 1 recognizes the address @S1 and walks back the datagram's application field towards the telnetd application of server device 1. Telnetd application of server device 1 sends the following message to the Telnet application on interconnection device 4 on its way back:

Trying...

Connected to 192.90.249.124.

Escape character is '^'.

*\$\$ 0000 *DNS-E V3U1.000 P1.001 P2.019 P3.010*IMA:BX77SIM 1988/10/21 17:23**

[0049]

This message is resent towards the Telnet application of client device 12 by telnetd application of interconnection device 4. Display of the above message on the terminal of client device 12 indicates that the message is in a DNS system and that it will reach server device 1. However, the application field of the datagram walks back the application layer of relay device 4 transparent to client device 12.

[0050]

The above method in manual operation can be implemented by a program that is executed by the application layer of interconnection device 4.

[0051]

The destination datagram of server device 1 that passes through the IP layer of interconnection device 4 walks back the application layer of interconnection device 4, for address @S1 is associated with the physical interface of interconnection device 4. In order to avoid clashing with server device 1 on network 3, it is better not to connect address @S1 to interface 14. By referring to drawing 3, address @S1 can be associated with a physical interface other than interface 19, such as physical interface 20, for example.

[0052]

A special processing example by relay application 22, which is described here, has a special advantage. When an encryption key is associated with address @S1 to encrypt the request from client device 12 and response to client device 12, interconnection device 4 will be able to decrypt the request and encrypt the response. The data can be circulated without any danger by getting decrypted on server network 3. Therefore, encryption and decryption resources are concentrated on interconnection device 4, and resources that can be used for server functions are left on server device 1 as much as possible. Relay application 22 can also encrypt the response once again before sending it on network 13.

[Brief Description of Drawings]

[Drawing 1]

This drawing shows an example of an interconnection device that has two physical interfaces.

[Drawing 2]

This drawing shows an example of a datagram.

[Drawing 3]

This drawing shows an example of an interconnection device that has three physical interfaces.

Fig.1

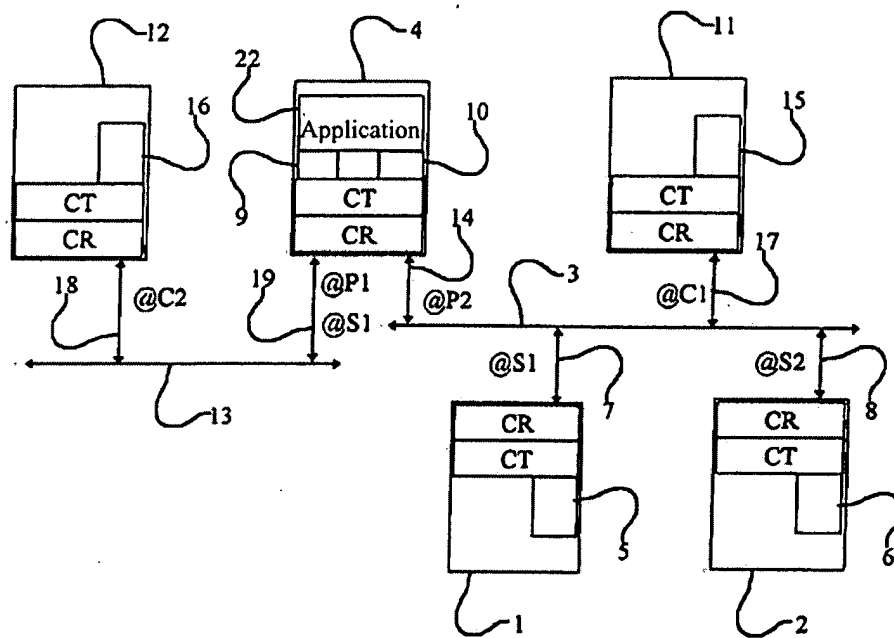


Fig.2

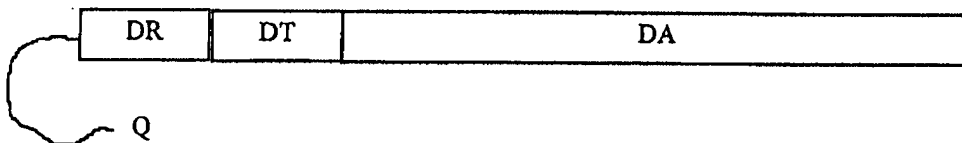
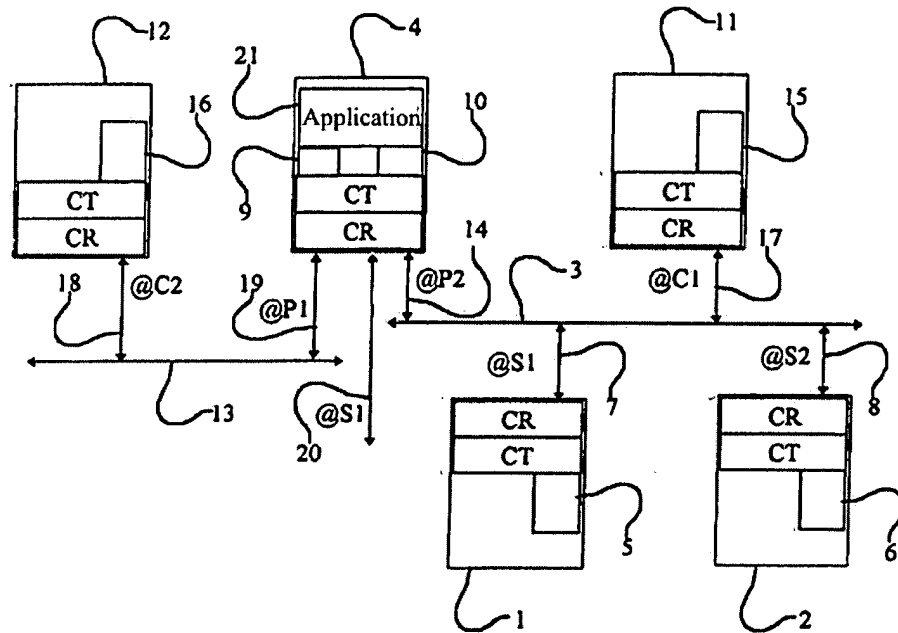


Fig.3



(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2003-509969

(P2003-509969A)

(43) 公表日 平成15年3月11日 (2003.3.11)

(51) Int.Cl.⁷

H 0 4 L 12/46

識別記号

1 0 0

F I

H 0 4 L 12/46

テマコード^{*} (参考)

1 0 0 Z 5 K 0 3 3

審査請求 有 予備審査請求 未請求 (全 23 頁)

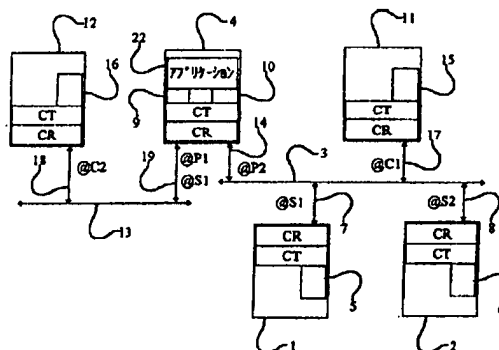
(21) 出願番号 特願2001-524324 (P2001-524324)
(86) (22) 出願日 平成12年9月7日 (2000.9.7)
(85) 翻訳文提出日 平成13年5月15日 (2001.5.15)
(86) 国際出願番号 PCT/FR00/02469
(87) 国際公開番号 WO01/020870
(87) 国際公開日 平成13年3月22日 (2001.3.22)
(31) 優先権主張番号 99/11594
(32) 優先日 平成11年9月16日 (1999.9.16)
(33) 優先権主張国 フランス (FR)
(81) 指定国 EP (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), CN, JP, KR, SG, US, VN

(71) 出願人 ブル・エス・アー
フランス国、エフ-78434・ループシエンヌ、ルート・ドウ・ベルサイユ、68
(72) 発明者 デュジオン、ジャン-イブ
フランス国、エフ-78580・モール、アブニユ・バストゥール、27・ビス
(72) 発明者 マルタン、ルネ
フランス国、エフ-91440・ビュール・シユール・イベツト、リュ・ゴメス、32
(74) 代理人 弁理士 川口 義雄 (外1名)
Fターム (参考) 5K033 BA04 CB09 DA05 DB19 EC03

(54) 【発明の名称】 クライアントネットワークに対してトランスペアレントな、サーバネットワークへのアクセス中継

(57) 【要約】

本発明は、第一の物理インターフェース19によりクライアントネットワーク13に結合され、第二の物理インターフェース14によりサーバネットワーク3に結合される相互接続装置4に関する。相互接続装置4は、クライアントネットワーク13からサーバ装置1、2に宛てられたデータグラムを受信するとともに、サーバネットワーク3へサーバ装置1、2に宛てられたデータグラムを送信する第一の中継アプリケーション22を含む。サーバネットワーク3に結合されるサーバ装置1、2のネットワーク間プロトコルアドレス@S1、@S2は、第一の物理インターフェース19に関連付けられるので、相互接続装置でアプリケーションレベルに遷るデータグラムは、クライアントネットワーク13でトランスペアレントに中継アプリケーションに利用提供される。



【特許請求の範囲】

【請求項1】 第一の物理インターフェース（19）によりクライアントネットワーク（13）に結合され、第二の物理インターフェース（14）によりサーバネットワーク（3）に結合される相互接続装置（4）であって、サーバネットワーク（3）に結合されるサーバ装置（1、2）の、相互接続装置（4）とは異なる少なくとも一つのネットワーク間プロトコルアドレス（@S1、@S2）が、第一の物理インターフェース（19）に関連付けられ、クライアントネットワーク（13）からサーバ装置（1、2）に宛てられたデータグラムを受信し、サーバネットワーク（3）へサーバ装置（1、2）に宛てられたデータグラムを送信する第一の中継アプリケーション（22）を含むことを特徴とする相互接続装置（4）。

【請求項2】 第一の物理インターフェース（19）によりクライアントネットワーク（13）に結合され、第二の物理インターフェース（14）によりサーバネットワーク（3）に結合される相互接続装置（4）であって、サーバネットワーク（3）に結合されるサーバ装置（1、2）の、相互接続装置（4）とは異なる少なくとも一つのネットワーク間プロトコルアドレス（@S1、@S2）が、第一の物理インターフェース（19）および第二の物理インターフェース（14）とは異なる第三の物理インターフェース（20）に関連付けられ、クライアントネットワーク（13）からサーバ装置（1、2）に宛てられたデータグラムを受信し、サーバネットワーク（3）へサーバ装置（1、2）に宛てられたデータグラムを送信する第一の中継アプリケーション（22）を含むことを特徴とする相互接続装置（4）。

【請求項3】 前記アドレス（@S1、@S2）が、クライアントネットワーク（13）で相互接続装置（4）のベースアドレス（@P1）の同義アドレスとして、第一の物理インターフェース（19）に関連付けられることを特徴とする請求項1に記載の相互接続装置（4）。

【請求項4】 相互接続装置（4）においてクライアントネットワーク（13）とサーバネットワーク（3）との間で中継アプリケーション（22）を実行し、該中継アプリケーションによって、クライアントネットワーク（13）でク

クライアントアプリケーション（１６）が、相互接続装置（４）とは異なるサーバネットワーク（３）のアドレス（@S１）のサーバ装置（１）宛てに送信するデータグラムを処理可能にする方法であって、中継アプリケーション（２２）が、データグラムを処理可能にするために前記クライアントアプリケーション（１６）を構成あるいは前記クライアントアプリケーションに情報伝達しなくても前記データグラムを受信するように、サーバネットワーク（３）に結合されない相互接続装置（４）の物理インターフェース（１９、２０）に前記アドレス（@S１）を関連付ける第一のステップを含むことを特徴とする方法。

【請求項５】 第一のステップが、サーバ装置（１）宛てにクライアントネットワーク（１３）で伝送されるデータグラムを、相互接続装置（４）に向けてルーティングする第二のステップに先行されることを特徴とする請求項４に記載の方法。

【請求項６】 中継アプリケーション（２２）が、クライアントネットワーク（１３）から送られる暗号化メッセージをサーバネットワーク（３）で解読して伝送するように、暗号化キーを有することを特徴とする請求項１または２に記載の相互接続装置（４）。

【請求項７】 中継アプリケーション（２２）が、サーバネットワーク（３）から送られる暗号化されていないメッセージを、クライアントネットワーク（１３）で暗号化して伝送するように、暗号化キーを含むことを特徴とする請求項１または２に記載の相互接続装置（４）。

【発明の詳細な説明】

【0001】

本発明は、情報処理ネットワークの領域に関する。情報処理ネットワークは、遠隔装置に配分されたアプリケーションの実行を可能にする。これらの遠隔装置は、同一のネットワークまたは、相互接続装置により相互接続される異なる複数のネットワークに接続される。

【0002】

遠隔装置間のトランザクションは、監視状態にあるサーバアプリケーションに要求メッセージを送信するクライアントアプリケーションによって初期化される。クライアントアプリケーションは、要求メッセージへの応答メッセージの待機状態に置かれる。要求メッセージを受け取ると、サーバアプリケーションは、クライアントアプリケーションに送信する応答メッセージを生成する。ネットワーク層は、送信アプリケーションを収容する装置から受信アプリケーションを収容する装置まで、データグラムとして各メッセージを搬送することができる。トランスポート層は、送信アプリケーションとネットワーク層との間、次いでネットワーク層と受信アプリケーションとの間で、すなわち、たとえばクライアントアプリケーションからサーバアプリケーションへ、メッセージを搬送することができる。アプリケーション層は、この層に固有の環境におけるアプリケーションの実行に関する。

【0003】

装置が、物理的に同一のネットワークに結合されない場合、ネットワーク層のルーティングプロトコルが、たとえばIPアドレス等のネットワーク間プロトコルアドレスにより、送信装置から相互接続装置に、また相互接続装置から受信装置にデータグラムを送る。相互接続装置の通過時に、データグラムは、ネットワーク層のレベルに留まる。クライアント装置と相互接続装置との間のネットワークは、クライアントネットワークと称される。サーバ装置と相互接続装置との間のネットワークは、サーバネットワークと称される。

【0004】

本発明が特に関与する技術領域は、中継アプリケーションを収容するための相

互接続装置 (proxy) に関する。中継アプリケーションは、クライアントネットワークとサーバネットワークとの間で交換されるメッセージに処理を実施する際に有効である。しかしながら、最終受信装置宛のデータグラムは、当然のことながら、相互接続装置のアプリケーション層には遡らない。

【0005】

知られている従来技術によれば、送信アプリケーションは、最終受信アプリケーションに直接アドレスせずに、相互接続装置の中継アプリケーションにメッセージをアドレスし、メッセージに与える処理に応じて中継アプリケーションがメッセージを再送できるように、メッセージを送る最終アプリケーションはどれであるかを中継アプリケーションへのメッセージ内で示す。これは、たとえばインターネットブラウザ (browser) で行われており、ブラウザでは、所定のクライアントアプリケーションに対して、ネットワーク層のための相互接続装置のアドレスと、トランスポート層のための中継アプリケーションのポート番号とを宣言することが可能であるので、ブラウザは、サーバ装置のアドレスと、最終宛先アプリケーションのポート番号とを、中継アプリケーションにアドレスされるデータグラムに封入する。だが、このためには、対応してクライアント装置を構成するように、メッセージが通過する中継アプリケーションはどれかを知らなければならない。その結果、柔軟性が欠如し、こうした柔軟性の欠如は、限られた数のアプリケーションに対しては許容できるとしても、異なる多数のアプリケーションに対しては満足のいくものではない。

【0006】

インターネットアドレス `http://www.pmg.lcs.mit.edu/cgi-bin/rfc/view?1928` で得られる資料 RFC1928 は、プロトコル「SOCKS v5」を記載しており、通常、使用されるポート番号は1080である。「TCP protocol Tunneling in Web Proxy Servers」という名称で知られる解決方法に対しても同様に、中継アプリケーションへの第一の接続を設定し、中継装置を最終装置に接続する第二の接続を設定することが必要である。

【0007】

上記の欠点を解消するために、本発明の目的は、クライアントアプリケーションが、中継アプリケーションのサービスを使用しない場合に行えるように、サーバアプリケーションへの接続を簡単に設定可能にし、従って、中継アプリケーションのサービスの使用を、クライアントアプリケーションに対してトランスペアレントにすることにある。

【0008】

本発明の第一の目的は、第一の物理インターフェースによりクライアントネットワークに結合され、第二の物理インターフェースによりサーバネットワークに結合される相互接続装置にあり、サーバネットワークに結合されるサーバ装置の少なくとも一つのネットワーク間プロトコルアドレスが、第一の物理インターフェースに関連付けられ、クライアントネットワークからサーバ装置に宛てられたデータグラムを受信し、サーバネットワークへサーバ装置に宛てられたデータグラムを送信する第一の中継アプリケーションを含むことを特徴とする。

【0009】

かくして、データグラムが、宛先アドレスとしてサーバ装置の相互ネットワークプロトコルアドレスを備える第一の物理インターフェースに到達すると、相互接続装置は、そのネットワーク層により、データグラムの宛先装置であるものとして認識される。相互接続装置のネットワーク層は、その場合、設定されたプロトコルを単に遵守することにより、相互接続装置のアプリケーション層に向かってデータグラムを遡る。このデータグラムを受け取ると、中継アプリケーションは、これを処理し、その後サーバ装置に再送することもあり、あるいは再送しないこともある。これは、クライアントアプリケーションに対して完全にトランスペアレントである。

【0010】

本発明の変形実施形態の目的は、第一の物理インターフェースによりクライアントネットワークに結合され、第二の物理インターフェースによりサーバネットワークに結合される相互接続装置にあり、サーバネットワークに結合されるサーバ装置の少なくとも一つのネットワーク間プロトコルアドレスが、第一の物理インターフェースおよび第二の物理インターフェースとは異なる第三の物理インタ

ーフェースに関連付けられ、該相互接続装置が、クライアントネットワークからサーバ装置に宛てられたデータグラムを受信し、サーバネットワークへサーバ装置に宛てられたデータグラムを送信する第一の中継アプリケーションを含む。

【0011】

ここで、ネットワーク層のプロトコルは、宛先アドレスを、データグラムを受信する第一の物理インターフェースではなく、相互接続装置の任意の一つの物理インターフェースに割り当てて、相互接続装置のアプリケーション層に向かって遡るようにしている。

【0012】

相互接続装置が、たとえばルーティングプロトコルに有効なベースアドレスを既にクライアントネットワークに有する場合、前記サーバ装置のアドレスは、クライアントネットワークで、相互接続装置のベースアドレスの同義アドレスとして、第一の物理インターフェースに関連付けられる。

【0013】

本発明の第二の目的は、相互接続装置においてクライアントネットワークとサーバネットワークとの間で中継アプリケーションを実行し、この中継アプリケーションによって、クライアントネットワークで、クライアントアプリケーションが、サーバネットワークに一個のアドレスを有するサーバ装置宛てに送信するデータグラムを処理可能にする方法にあり、中継アプリケーションが前記データグラムを受信するように、サーバネットワークに結合されない相互接続装置の物理インターフェースに、サーバネットワークで前記アドレスに関連付ける第一のステップを含むことを特徴とする。

【0014】

これは、中継アプリケーションがデータグラムを処理可能にするために前記クライアントアプリケーションを構成したり、あるいは前記クライアントアプリケーションに情報伝達したりする必要がないという長所を有する。実際、クライアントアプリケーションは、サーバ装置のアドレスを使用することによりデータグラムを送信し続ける。データグラムが相互接続装置の第一の物理インターフェースに到着すると、ネットワークプロトコルは、当然、相互接続装置のアプリケー

ション層に向かってデータグラムが遡るようにし、それによって中継アプリケーションがデータグラムを受信可能になる。

【0015】

クライアントネットワークからサーバネットワークに伝送されるデータグラムを、相互接続装置によりルーティングしなければならない場合、この方法は、サーバ装置宛てにクライアントネットワークで伝送されるデータグラムを相互接続装置にルーティングする第二のステップが、第一のステップよりも先行することの特徴とする。これは、たとえば、クライアントネットワークとサーバネットワークとの間の相互接続装置が一個ではない場合である。

【0016】

本発明の実施形態の他の長所および詳細は、添付図面に関する以下の説明から明らかになるであろう。

【0017】

図1は、サーバ装置1、2、クライアント装置11、12を示している。装置1、2、11は、個々の物理インターフェース7、8、17によりサーバネットワーク3に接続されている。クライアント装置12は、物理インターフェース18によりクライアントネットワーク13に接続される。ネットワーク3、13は、物理的に異なる。相互接続装置4は、物理インターフェース14によりサーバネットワーク3に、物理インターフェース19によりネットワーク13に接続されている。

【0018】

装置1、2、11、12で実行されるアプリケーション5、6、15、16は、プロトコルに応じてUDP等の非接続モードまたはTCP等の接続モードで、トランスポート層CTにより相互に通信する。トランスポート層CTは、IP等のプロトコルに応じてネットワーク層CRを監視する。

【0019】

ネットワーク層CRでは、装置1がアドレス@S1により認識され、装置2は、アドレス@S2により認識され、装置11は、アドレス@C1により認識される。知られているように、各アドレス@S1、@S2、および@C1は、ネット

ワーク3を識別する共通値を持つネットワークフィールドと、ネットワーク3に結合される各装置を識別する別個の値を持つ装置フィールドとを有する。装置12は、ネットワーク13を識別するネットワークフィールド値と、ネットワーク13で装置12を識別する装置フィールド値とを持つアドレス@C2により認識される。相互接続装置4は、ネットワーク13を識別するネットワークフィールド値、およびネットワーク13で相互接続装置4を識別する装置フィールド値を持つアドレス@P1と、ネットワーク3を識別するネットワークフィールド値、およびネットワーク3で相互接続装置4を識別する装置フィールド値を持つアドレス@P2とにより認識される。

【0020】

装置は、データグラムとしてネットワークで循環するメッセージにより相互に通信する。図2は、データグラムの一例を示す。連続ビットフレームから構成されるこのデータグラムは、主に3個の連続フィールドから構成される。第一のフィールドDRは、ネットワーク層のプロトコル用である。第二のフィールドDTは、ネットワーク層を監視するトランスポート層のプロトコル用である。第三のフィールドDAは、トランスポート層を監視するアプリケーション層用である。たとえばwebにおける要求の場合、フィールドDRが送信元と宛先のIPアドレスを含み、フィールドDTが送信元と宛先のTCPポート番号を含み、フィールドDAがHTTPデータを含む。

【0021】

たとえば、クライアント装置11で実行されるクライアントアプリケーション15が、サーバ装置1に配置されるサーバアプリケーション5によって処理されるファイルへのアクセス要求を実行する場合、アプリケーション5は、クライアント装置11の層CTにその要求を伝送し、層CTは、フィールドDAに要求を書き込むとともに、フィールドDTに、アプリケーション15用のサービスポート番号とアプリケーション5用のサービスポート番号とを書き込む。クライアント装置11の層CTは、フィールドDT、DAを装置11の層CRに伝送し、層CRは、クライアント装置11のアドレス@C1とサーバ装置1のアドレス@S1とをフィールドDRに書き込む。次に、層CRは、このように構成されたデー

タグラムを、サーバ装置1のインターフェース7に到着するインターフェース17に伝送する。サーバ装置1の層CRは、アドレス@S1により、データグラムがサーバ装置1の上層宛てであることを認識し、フィールドDT、DAを装置1の層CTに再送する。層CTは、アプリケーション5用のサービスポート番号により、フィールドDAをアプリケーション5に再送し、アプリケーション5が要求を処理する。

【0022】

クライアント装置12で実行されるアプリケーション16が、サーバ装置1に配置されるアプリケーション5により処理されるファイルにアクセス要求を行う場合、アプリケーション16は、クライアント装置12の層CTにその要求を伝送し、層CTは、フィールドDAにこれを書き込むとともに、フィールドDTに、アプリケーション16用のサービスポート番号と、アプリケーション5用のサービスポート番号とを書き込む。クライアント装置12の層CTは、フィールドDT、DAをクライアント装置12の層CRに伝送し、層CRは、クライアント装置12のアドレス@C2とサーバ装置1のアドレス@S1とをフィールドDRに書き込む。次に、層CRは、このように構成されたデータグラムを、ネットワーク13と3の間のルータとして宣言される、相互接続装置4のインターフェース19に到着するインターフェース18に伝送する。

【0023】

本発明による装置がない場合、アドレス@S1は、相互接続装置4宛てのアドレスではないので、相互接続装置4の層CRは、データグラムが相互接続装置4の上位層宛てではないことを認識する。その場合、相互接続装置4の層CRは、アドレス@S1のネットワークフィールドと同じ値を含む行をルーティングテーブル内で探す。このようにして見つかった行は、ネットワーク3へのアクセスインターフェースであるものとしてインターフェース14を示す。相互接続装置4の層CRは、インターフェース14によりネットワーク3にデータグラムを再送し、その結果、データグラムがサーバ装置1のインターフェース7に到着する。サーバ装置1の層CRは、アドレス@S1により、データグラムがサーバ装置1の上位層宛てであることを認識し、フィールドDT、DAをサーバ装置1の層C

Tに再送する。アプリケーション5用のサーバポート番号により、層CTは、アプリケーション5にフィールドDAを再送し、このアプリケーションが要求を処理する。

【0024】

本発明による装置では、相互接続装置4が、ネットワーク13から送られる要求のために中継サーバ(proxy server)の役割を果たすアプリケーション22を含む。アプリケーション22は、複数の長所を有し、たとえば、サーバネットワーク3に接続される装置1、2、11へのアクセス制御を実施可能である。また、キャッシュ(cache)メモリにある先行要求への応答を保護し、サーバ装置1、2まで新しい要求を送る必要なく、これらの新しい要求への応答を再生することができる。

【0025】

層CRの複数のアドレスは、物理インターフェース19、通常アドレス@S1、およびネットワーク3に接続されるサーバ装置1の通常アドレス@P1に関連付けられる。また、サーバ装置2のアドレス@S2を物理インターフェース19に関連付けることもできる。後述するように、クライアントネットワークが中継アプリケーション22のサービスの使用を決定する従来技術とは異なり、ここでは、サーバネットワークが、物理インターフェース19にアドレス@S1に関連付けることにより、このような利用、たとえばサーバ1へのアクセスを決定する。

【0026】

アプリケーション22は、アプリケーション5の入力ポートと同じ番号の入力ポート9と、出力ポート10とを含み、この出力ポートに一つの番号を割り当て、アプリケーション5宛ての任意の要求メッセージを管理することができる。

【0027】

こうした特別の装置により、クライアント装置12は、相互接続装置4との間接続を設定したことを知る必要がない。クライアント装置12で実行されるアプリケーション16が、サーバ装置1に配置されるアプリケーション5宛ての要求を実行する場合、アドレス@S1は、今や相互接続装置4のアドレスとしてネ

ットワーク13で認識される。

【0028】

アプリケーション5宛ての要求を実行するために、アプリケーション16は、ネットワーク13でのデータグラムQを送る。データグラムQは、フィールドCRにアドレス@S1、@S2を含み、トランスポートフィールドにアプリケーション5および16のポート番号を含み、フィールドCAにアプリケーション5宛ての最終情報を含む。

【0029】

相互接続装置4の物理インターフェース19でデータグラムQを受信すると、相互接続装置4のネットワーク層CRは、フィールドDRにおける宛先アドレス@S1を固有のアドレスであるものとして認識し、相互接続装置4のトランスポート層CTに向かってデータグラムを遡る。トランスポート層CTは、アプリケーション22のポート番号9であるものとしてフィールドDT内の宛先番号を認識し、このアプリケーションにデータグラムQの内容を伝送する。

【0030】

アプリケーション22は、データグラムQのフィールドDAの内容を処理する。アプリケーション22によるデータグラムQの処理は、たとえばアクセス権をチェックすることや、サーバアプリケーション5にデータグラムQを伝える、もしくは伝えない決定を下すために、相互接続装置4が、そのキャッシュメモリに要求に対する応答を既に含むかどうかチェックすることからなる。

【0031】

クライアントアプリケーション16から送られる要求メッセージを処理するために、アプリケーション22が、アプリケーション5に要求メッセージを送信する必要がある場合、アプリケーション22は、相互接続装置4のトランスポート層CTに後続データ、すなわち、フィールドDAに置かれる要求の内容、アプリケーション5の入力ポート番号、要求への回答を管理するためのアプリケーション22の出力ポート番号、サーバ装置1のネットワーク間プロトコルアドレス@S1を知らせる。これらのデータは、相互接続装置4のネットワーク層CRに伝達される。これらのデータを受信すると、相互接続装置4のネットワーク層CR

は、そのルーティングテーブルで、アドレス@S 1のネットワークフィールドに応じて、どのネットワークでデータグラムを送信するか探す。ここで記載した例では、アドレス@S 1のネットワークフィールドは、サーバ装置1が接続されるネットワーク3に対応するので、層CRは、物理インターフェース14に向けて、宛先アドレス@S 1と、物理インターフェース14に関連付けられる送信元アドレス@P 2とをフィールドDRに含むデータグラムを送信する。データグラムは、サーバ装置1とサーバ装置1のサーバアプリケーション5まで、クライアントサーバ3により従来の方法で到達する。

【0032】

インターフェース14でアプリケーション5が受信する応答は、アドレス@P 2が相互接続装置4のアドレスであるので、ネットワーク層によってアプリケーション22に廻り、また、応答用のポート番号はアプリケーション22がポート10に割り当てる番号であるので、トランスポート層CTによりアプリケーション22に廻る。要求および応答を管理する内部機構を用いて、アプリケーション22は、アプリケーション16から受信した出力ポート番号に応答に関連付ける。アプリケーション22は、応答をアプリケーション16に再送するために、相互接続装置4のトランスポート層CTに後続データを知らせる。すなわち、フィールドDAに置かれる応答の内容、アプリケーション16の出力ポート番号、要求への応答を管理するためにアプリケーション5の入力ポート番号と同じであるアプリケーション22の入力ポート番号、クライアント装置12の宛先ネットワーク間プロトコルアドレス@C 2、およびサーバ装置1の送信元ネットワーク間プロトコルアドレス@S 1である。これらのデータは、トランスポート層により相互接続装置4のネットワーク層CRに伝送される。相互接続装置4のネットワーク層CRは、上記データを受信すると、そのルーティングテーブルで、アドレス@C 2のネットワークフィールドに応じて、どのネットワークでデータグラムを送信するか探す。ここで記載した例では、アドレス@SC 2のネットワークフィールドは、クライアント装置12が接続されるネットワーク13に対応するので、層CRは、宛先アドレス@P 2と、物理インターフェース19に関連付けられる送信元アドレス@S 1とを、フィールドDRに含むデータグラムを、物理イ

ンターフェース19に送信する。データグラムは、クライアント装置12とクライアント装置12のクライアントアプリケーション16まで、クライアントネットワーク13により従来の方法で到達する。

【0033】

かくして、クライアント装置12のアプリケーション16は、アプリケーション22を通過することなく、サーバ装置1内のアプリケーション5からの応答を戻す。アプリケーション22の通過は、クライアントアプリケーション16に対してトランスペアレントに行われている。

【0034】

図3を参照すると、アドレス@S1は、前述のようなインターフェース14ならびに、ここでは特にインターフェース19とは異なる物理インターフェース20に関連付けられる。

【0035】

データグラムがアドレス@S1を持つネットワーク13で送信されると、相互接続装置4のネットワーク層CRのルーティングプロトコルは、アドレス@P1が関連付けられるインターフェース19でデータグラムを受信する。物理インターフェース20に関連付けられるアドレス@S1は、相互接続装置4のアドレスであるので、データグラムは、相互接続装置4のアプリケーション層CAに遡る。

【0036】

中継アプリケーション21は、前述の中継アプリケーション22と同様に、受信データグラムから送られる要求メッセージを処理する。応答メッセージをクライアント装置12に送信するために、中継アプリケーション22は、物理インターフェース20が結合されるバーチャルネットワークに向けて特にパイロットを提供する。

【0037】

本発明の実施を容易にするには、IPアドレス@S1がインターフェース19に結合される場合が特に有利である。以下の簡単な例では、アプリケーション16が、クライアントアプリケーションとしてのTelnet機能を実行し、中継

アプリケーション22が、アプリケーション16のサーバアプリケーションとしてのtelnetd機能と、アプリケーション5のクライアントとしてのTelnet機能を実行する。アプリケーション5は、中継アプリケーション22のサーバとしてtelnetd機能を実行する。Telnetおよびtelnetdは、Telnet機能が実行されるクライアント装置の端末を、telnetd機能が実行されるサーバ装置に接続する、TCP/IPを用いた知られている機能である。

【0038】

各装置は、コマンドを実行する装置に従うように、異なるオペレーションシステムに向かう。クライアント装置12は、バージョン4.1のAIXシステム（登録商標）に向かい、IPアドレスとして@C1=129.182.51.58を有する。中継装置4は、バージョン4.2のAIXシステムに向かい、IPアドレスとして@P1=129.182.51.21と、@P2=192.90.249.22を有する。サーバ装置12は、DNS-E装置（専用）に向かい、IPアドレスとして@S1=192.90.249.124を有する。ネットワーク13は、IPアドレス@R1=129.182.50、マスク@M1=255.255.254.0により、知られている方法でアクセス可能である。

【0039】

クライアント装置12において、次のコマンド

```
route add-host 192.90.249.124 129.182.51.21
```

は、送信データグラムが、アドレス@S1のサーバ装置1に到達するために、アドレス@P1の中継装置を通過することを決定する。

【0040】

サーバ装置1において、次のコマンド

```
route add-net 129.182.50 192.90.249.22-netmask 255.255.254.0
```

は、送信データグラムが、アドレス@R1のネットワーク13のあらゆる装置に到達するために、アドレス@P2の中継装置を通過することを決定する。

【0041】

クライアント装置12において、次のコマンド

```
Telnet 192.90.249.124
```

は、アドレス@S1のサーバ装置1に到達するために、Telnetアプリケーションを作動する。この段階で、IPアドレス@S1により認識される唯一の装置は、サーバ装置1である。相互接続装置4のIP層は、サーバ装置1のIP層に向かって、クライアント装置12のIP層から送られるデータグラムをルーティングする。サーバ装置1のIP層は、アドレス@S1を認識し、サーバ装置1のtelnetdアプリケーションに向かってデータグラムのアプリケーションフィールドを遡る。サーバ装置1のtelnetdアプリケーションは、復路でクライアント装置12に次のメッセージを送る。

```
Trying...
```

```
Connected to 192.90.249.124.
```

```
Escape character is '^]'.
```

```
$$ 0000 *DNS-E V3U1.000 P1.001 P2.0  
19 P3.010* IMA:BX77SIM 1988/10/21 17:  
23*
```

【0042】

クライアント装置12の端末における上記メッセージの表示は、このメッセージがDNSシステムの環境にあり、すなわちサーバ装置1に直接到達することを示している。中継装置4を通過するのは、IPルーティングを実施する場合だけである。

【0043】

クライアント装置12では、次のコマンド

```
Telnet 129.182.51.21
```

が、アドレス@P1の中継装置4に到達するためにTelnetアプリケーションを作動する。相互接続装置4のIP層はアドレス@P1を認識し、中継装置4のtelnetdアプリケーションに向かってデータグラムのアプリケーションフィールドを遡る。相互接続装置4のtelnetdアプリケーションは、復路

でクライアント装置12に次のメッセージを送信する。

```
Trying...
Connected to 129.182.51.21.
Escape character is '^]'.
Telnet (treize)
AIX Version 4
(c) Copyrights by IBM and by others
1982, 1996.
Login:
【0044】
```

クライアント装置12の端末における上記メッセージの表示は、このメッセージがAIXシステムの環境にあり、すなわち相互接続装置4に到達することを示している。これにより、相互接続装置4で実行されるクライアント装置12の端末からのコマンドを管理可能になる。

【0045】

相互接続装置4では、インターフェース19がen1と称されて、次のコマンド

```
ifconfig en1 192.90.249.124 alias
```

が、インターフェース19に関連付けられる追加アドレスとしてアドレス@S1を決定する。相互接続装置4は、ネットワーク13でIP層によりサーバ装置1と混同されるおそれはない。何故なら、ネットワーク13は、ネットワーク3とは物理的に異なるからである。同様に、次のコマンド

```
ifconfig en1 192.90.249.125 alias
```

は、インターフェース19に関連付けられる追加アドレスとしてアドレス@S2を決定する。

【0046】

クライアント装置12に戻ると、次のコマンド

```
Telnet 192.90.249.124
```

が、上記とは異なる効果を持つTelnetアプリケーションを作動する。クラ

クライアント装置12の端末に表示されるメッセージは、次の通りである。

```
Trying...
Connected to 129.182.51.21.
Escape character is '^]'.
Telnet (treize)
AIX Version 4
(c) Copyrights by IBM and by others
1982, 1996.
Login:
【0047】
```

クライアント装置12の端末における上記メッセージの表示は、このメッセージが、相互接続装置4のAIXシステムの環境にあることを示す。アドレス@S1により、サーバ装置1のtelnetdアプリケーションへの接続を求めたにもかかわらず、コマンドは、相互接続装置4のtelnetdアプリケーションへの接続を実行したわけである。これは、相互接続装置4のIP層が、ネットワーク3へのルーティングを考慮せずに、相互接続装置4に固有の宛先アドレスとしてアドレス@S1を認識したことによって説明される。従って、相互接続装置4のIP層は、相互接続装置4のtelnetdアプリケーションに向かって、インターフェース19で受信したデータグラムのアプリケーションフィールドを遡る。

【0048】

相互接続装置4では、次のコマンド

```
Telnet 192.90.249.124
```

が、アドレス@S1のサーバ装置1に到達するために、Telnetアプリケーションを作動する。この段階では、インターフェース14からIPアドレス@S1により認識される唯一の装置が、サーバ装置1である。サーバ装置1のIP層は、アドレス@S1を認識し、サーバ装置1のtelnetdアプリケーションに向かってデータグラムのアプリケーションフィールドを遡る。サーバ装置1のtelnetdアプリケーションは、復路で相互接続装置4のTelnetアプ

リケーションに向かって、次のメッセージを送信する。

```
Trying...
Connected to 192.90.249.124.
Escape character is '^]'.
$$ 0000 *DNS-E V3U1.000 P1.001 P2.0
19 P3.010* IMA:BX77SIM 1988/10/21 17:
23*
```

【0049】

このメッセージは、クライアント装置12のTelnetアプリケーションに向かって相互接続装置4のtelnetdアプリケーションにより再送される。クライアント装置12の端末におけるこのメッセージの表示は、メッセージが、DNSシステム的环境にあり、サーバ装置1に到達することを示す。しかしながら、データグラムアプリケーションフィールドは、クライアント装置12に対してトランスペアレントに、中継装置4のアプリケーション層を遡る。

【0050】

マニュアル操作による上記の方法は、相互接続装置4のアプリケーション層により実行されるプログラムによって実施可能である。

【0051】

相互接続装置4のIP層を通過するサーバ装置1の宛先データグラムは、アドレス@S1が相互接続装置4の物理インターフェースに関連付けられるので、相互接続装置4のアプリケーション層を遡る。ネットワーク3においてサーバ装置1との衝突を避けるために、アドレス@S1をインターフェース14に結合しないことが好ましい。図3を参照すると、アドレス@S1を、インターフェース19以外の物理インターフェース、たとえば物理インターフェース20に関連付けることができる。

【0052】

ここで記載した中継アプリケーション22による特別な処理例は、特別な長所を有する。暗号化キーをアドレス@S1に関連付け、クライアント装置12からの要求およびクライアント装置12宛ての応答を暗号化する場合、要求の暗号解

除および応答の暗号化が、相互接続装置4によって実施可能になる。データは、危険を冒さずにサーバネットワーク3で暗号解除されて循環することができる。このため、暗号化リソースおよび暗号解除リソースを相互接続装置4に集中し、サーバ機能のために使用可能なリソースをサーバ装置1に最大限残す。中継アプリケーション22はまた、ネットワーク13で送信する前に応答を再度、暗号化することができる。

【図面の簡単な説明】

【図1】

2個の物理インターフェースを備えた相互接続装置の一例を示す図である。

【図2】

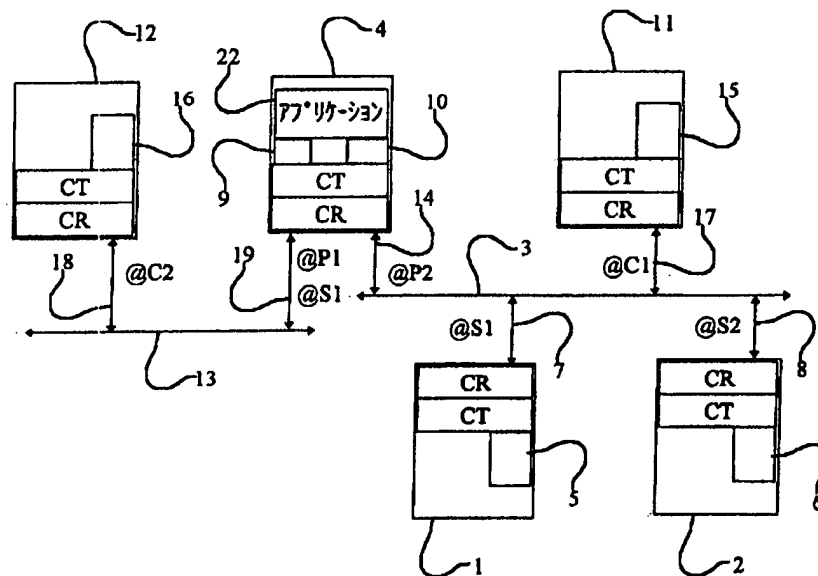
データグラムの一例を示す図である。

【図3】

3個の物理インターフェースを備えた相互接続装置の一例を示す図である。

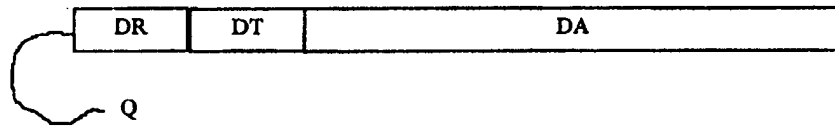
【図1】

Fig.1



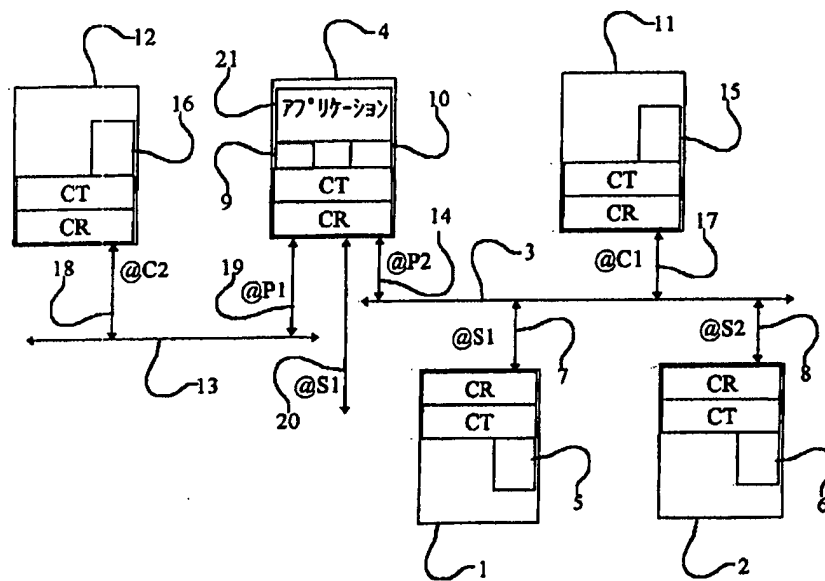
【図2】

Fig.2



【図3】

Fig.3



【国際調査報告】

INTERNATIONAL SEARCH REPORT

Internat'l Application No. PCT/FR 00/02469	
A. CLASSIFICATION OF SUBJECT MATTER IPC 7 H04L29/06 H04L29/12	
According to International Patent Classification (IPC) or to both national classification and IPC	
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 7 H04L	
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched	
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal, PAJ	
C. DOCUMENTS CONSIDERED TO BE RELEVANT	
Category *	Citation of document, with indication, where appropriate, of the relevant passages Relevant to claim No.
X	EP 0 713 311 A (MILKYWAY NETWORKS CORP) 22 May 1996 (1996-05-22)
Y	page 4, line 48-58 page 6, line 16 -page 7, line 54 page 8, line 46-53 page 9, line 12-25
A	US 5 898 830 A (COLEY CHRISTOPHER D ET AL) 27 April 1999 (1999-04-27)
Y	column 4, line 17-52 column 7, line 41 -column 9, line 35 column 11, line 36 -column 12, line 27 column 14, line 66 -column 15, line 46
	1,2 6,7 1,2,4 6,7
<input type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.	
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principles or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "A" document member of the same patent family	
Date of the actual completion of the international search	Date of mailing of the international search report
13 October 2000	20/10/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentplan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tr. 31 851 ext. 1 Fax: (+31-70) 340-2010	Authorized officer Dupuis, H

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern. Appl. No.

PCT/FR 00/02469

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0713311 A	22-05-1996	CA 2136150 A	19-05-1996
		US 5623601 A	22-04-1997
US 5898830 A	27-04-1999	US 6052788 A	18-04-2000